Commun Nonlinear Sci Numer Simulat 19 (2014) 905–913

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

# A one-way coupled chaotic map lattice based self-synchronizing stream cipher

Shihong Wang [a,b,*], Gang Hu [c], Hu Zhou [a]

[a] School of Sciences, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[c] Department of Physics, Beijing Normal University, Beijing 100875, China

ARTICLE INFO

*Article history:*
Received 22 February 2013
Accepted 17 August 2013
Available online 25 August 2013

*Keywords:*
Coupled map lattice
Chaos
Self-synchronizing stream ciphers

ABSTRACT

Self-synchronizing stream cipher (SSSC) has the advantage that the receiver can automatically synchronize with the sender after receiving previously transmitted ciphertext. However, it has also serious difficulty to keep security due to its self-synchronizing structure. In this paper, a new SSSC based on one-way coupled chaotic map lattice is proposed. By combining floating-point chaotic computations with algebraic operations, the cipher has high bit confusion and diffusion rates. It has both advantages of robustness of synchronization and strong security. The cipher can serve as a new type of SSSC candidate in software implementation.



## 1. Introduction

In the past two decades, the application of chaos to cryptology has become a promising direction due to some favorable chaotic characteristics such as random-like behavior, nonperiodicity and the sensitivity of chaotic trajectories to initial conditions and control parameters. Many cryptosystems based on chaos are proposed, including pseudo-random number generators, block ciphers, public ciphers, hash functions, image encryption systems and stream ciphers[1–8]. Some of them were applied in circuit, laser and commercial fibre-optic communication systems [3,7,8]. Since chaos synchronization was proposed by Pecora and Carrol [9], many chaos-based self-synchronizing stream ciphers (SSSCs) have been designed and investigated [10–14]. The disadvantages of low security and inefficiency limit applications of these chaotic SSSCs [15–20].

Stream ciphers are classified as synchronizing and self-synchronizing stream ciphers. Compared with block ciphers and synchronizing stream ciphers, SSSCs have an admiring advantage that the receiver can automatically synchronize with the sender after receiving previously transmitted ciphertext. Thus SSSCs can resist against bit slips and deletions, and be used in a channel such as low bit errors or no redundant bits are introduced for the purpose of synchronization. So far almost all of dedicated SSSCs have been proven to be insecure [21–30]. Thus, designing secure and effective SSSCs is still an open problem in cryptography.

In Refs. [31–34], authors suggested that using one-way coupled map lattice (OWCML) and some simple algebraic operations could enhance the security of chaotic SSSCs. For implementation efficiency, parallel encryption was used in the systems of [33,34]. Because chaos synchronization in the suggested OWCMLs SSSCs depends on all parameters of coupling strength, system size and other control parameters [31–34], and these SSSCs have disadvantage of great error propagation.

* Corresponding author at: School of Sciences, Beijing University of Posts and Telecommunications, Beijing 100876, China. Tel./fax: +86 0 1062282452.
*E-mail address:* shwang@bupt.edu.cn (S. Wang).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.08.024

In this paper, we will go further to apply the idea of OWCML to design a new SSSC. The system based on a new OWCML, with all advantages of spatiotemporal-chaos-based cryptography well kept, has less error propagation.

The paper is organized as follows. In Section 2, we present general structures of SSSCs and the reason why chosen-ciphertext attacks are powerful against SSSCs. Section 3 presents a new OWCML. In Section 4, we introduce a new chaos-based SSSC (CB-SSSC) that combines the chaotic computation of OWCML together with algebraic operations for the optimization of both security and performance. The design rationale of CB-SSSC is specified. In Section 5, we evaluate statistical properties of CB-SSSC. In Section 6, we specify the computational efficiency in software implementation. The last section presents conclusions.

## 2. Self-synchronizing stream ciphers and chosen-ciphertext attacks

The encryption and decryption of SSSC are shown in Fig. 1, where $p_t, c_t$ and $z_t$ are plaintext, ciphertext and keystream, respectively. The nonlinear function $W$ produces a keystream, $h$ and $h^{-1}$ represent encryption and decryption transformations (they are usually simple bitwise XOR). From the scheme we can see that the keystream depends on both a secret key $\mathbf{k}$ and a fixed amount of preceding ciphertext, i.e., the keystream has memories of the ciphertext, which is essentially different from synchronizing stream ciphers. Thus the keystream can be written as

$$z_t = W(\mathbf{k}, c_{t-m}, c_{t-m+1}, \ldots, c_{t-1}), \tag{1}$$

which is also called as a *canonical transformation*. If an error or a ciphertext lost happens, the errors of the receiver can propagate forward $m$ time steps. After $m$ consecutive correct ciphertext are received, the receiver re-synchronizes automatically with the sender. Thus, self-synchronizing is the distinguishing characteristics of SSSCs. However these characteristics cannot resist against the attacks of injections, deletions and replay of ciphertext.

According to the information accessible to an attacker, attacks are classified as ciphertext-only, plaintext-known, chosen-plaintext, and chosen-ciphertext attacks, among which chosen-ciphertext attacks are the strongest ones. From Eq. (1) we can see that keystream is only determined by a fixed number of previous ciphertexts (i.e., $z_t$ is unique determined by $c_{t-m}, c_{t-m+1}, \ldots, c_{t-1}$ through a function $W$), therefore chosen-ciphertext attacks are the most suitable attacks for SSSCs. To resist against chosen-ciphertext attacks and enhance the security of SSSCs, the canonical transformation must have sufficiently complicated operations. However, the complexity of the canonical transformation is restricted by implementation efficiency.

## 3. One-way coupled map lattices

We first consider a drive-response OWCML that is used in the cryptosystems of Refs. [31–34]. The dynamics of the driving system reads

$$x_t^i = (1-\varepsilon) f(x_{t-1}^i) + \varepsilon f(x_{t-1}^{i-1}), \quad i = 1, 2, 3, \ldots, L, \tag{2}$$

where $t = 1, 2, \ldots$ is the time index, $i = 1, 2, \ldots L$ is the map index, and $L$ is the size of the system. $\varepsilon$ is a coupling constant. The periodic boundary condition is used. We take Logistic map $f(x) = \mu x(1-x)$ as the local map, where $\mu \in [0, 4]$ and $x \in [0, 1]$. If $\mu > 3.57$, Logistic map is chaotic.

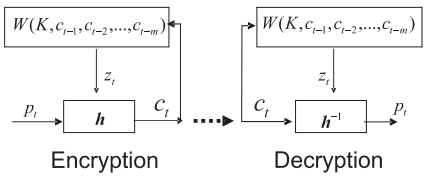


**Fig. 1.** The encryption and the decryption schemes of a SSSC.

**Table 1**
The average re-synchronizing time of Eqs. (2) and (3).

| | $L$ | | |
|---|---|---|---|
| $\varepsilon$ | 7 | 14 | 20 |
| 0.8500 | 36 | 45 | 48 |
| 0.9000 | 28 | 34 | 38 |
| 0.9900 | 12 | 14 | 16 |
| 0.9990 | 7 | 8 | 10 |
| 0.9999 | 6 | 7 | 8 |